



AF
\$IPW
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Arindam Das- PURKAYASTHA et al.) Examiner: Longbit CHAI
)
) Art Unit: 2131
Serial No.:	09/931,526)
) Our Ref: 618998-3 30006636-3 US
Filed:	August 16, 2001)
) Date: January 2, 2007
For:	"APPARATUS AND METHOD FOR ESTABLISHING TRUST")
) Re: <i>Appeal to the Board of Appeals</i>
)

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the non-Final rejection dated August 15, 2006, for the above identified patent application. Please charge the amount of \$500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief to deposit account no. 08-2025. Appellants submit that this Appeal Brief is being timely filed, since the Notice of Appeal was filed on November 14, 2006.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

01/09/2007 CNEGAI 00000062 002025 09931526
01 FC:1402 500.00 DA

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1 - 61 are the subject of this Appeal and are reproduced in the accompanying appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates generally to computer security, and more specifically to the establishment of a particular level of trust in a computer based upon the response of that computer to a challenge. Key to the present invention is the existence of a physically trusted device within the computer, that is, a device that is tamper-proof, and that is able to acquire and provide an integrity metric for the computer in response to a challenge (p. 5, ll. 3-8). The integrity metric provided by the trusted device is then compared with an integrity metric for the computer that is provided by a trusted party, and the challenger decided upon a level of trust to place in the computer based upon whether the two integrity metrics match, and optionally the scope of the integrity metric (p. 5, ll. 9-10). The integrity metric has values for a plurality of characteristics associated with the computer (claim 1), such as a digest of the BIOS instructions in the BIOS memory of the computer (p. 10, ll. 10-12). Preferably each component, but at least each critical component, of the computer has an integrity value associated with it, a so-called CCV (Component Configuration Value), that can be included in the integrity metric acquired by the trusted device of the computer (p. 10, l. 22 p. 11, l. 7). There are a number of ways the integrity metric may be calculated, all of which are contemplated by the invention (p. 15, l. 16 – p. 16, l. 32).

With greater particularity, the invention claimed in claim 1 is directed to a computer apparatus comprising a receiver for receiving an integrity metric for a computer entity (10) via a trusted device (24) associated with the computer entity, the integrity metric having values for a

plurality of characteristics associated with the computer entity, and a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric (p. 5 l. 3 – p. 9 l. 21, p. 17 l. 1 – p. 21 l. 23; Figs. 1-3, 5).

The invention claimed in claim 6 is directed to a method of assigning a trust level comprising receiving an integrity metric for a computer entity (10) via a trusted device (24) associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity, and assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric (p. 5 l. 3 – p. 9 l. 21, p. 17 l. 1 – p. 21 l. 23; Figs. 1-3, 5).

The invention claimed in claim 7 is directed to a method for establishing communications with a computer entity (10) comprising requesting (625) a trusted device (24) associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity, receiving (640) a response from the trusted device including an integrity metric calculated for the entity by the trusted device, comparing (670) values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party, and selecting a level of trust for the entity from a plurality of predefined levels of trusts based on at least one value in the integrity metric calculated for the entity by the trusted device (p. 5 l. 3 – p. 9 l. 21, p. 17 l. 1 – p. 21 l. 23; Figs. 1-3, 5).

The invention claimed in claim 24 is directed to a method for a computer entity (10) to respond to a request for integrity check prior to exchanging data comprising receiving (640) at a trusted device (24) associated with a computer entity a request to provide an integrity metric containing values indicative of one or more characteristics of the entity, calculating (630) at the trusted device values indicative of one or more characteristics of the entity, and providing (635) a response from the trusted device including an integrity metric including the values indicative of one or more characteristics of the entity (p. 5 l. 3 – p. 9 l. 21, p. 17 l. 1 – p. 21 l. 23; Figs. 1-3, 5).

The invention claimed in claim 42 is directed to a method for establishing communications between a computer entity (10) and a user comprising presenting (625) a

request from the user to a trusted device (24) associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity, presenting (635) to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device, comparing (670) at the user values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party, and selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device (p. 5 l. 3 – p. 9 l. 21, p. 17 l. 1 – p. 21 l. 23; Figs. 1-3, 5).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-9, 11-19, 24-26, 28-37, 40, 42-55 and 58 are patentable under 35 U.S.C. 102(e) over U.S. Pat. No. 6,678,833 to Grawrock (hereinafter “Grawrock”).

Issue 2: Whether claims 10, 27 and 45 are patentable under 35 U.S.C. 103(a) over Grawrock in view of U.S. Pat. No. 6,209,099 to Saunders (hereinafter “Saunders”).

Issue 3: Whether claims 20, 21, 38, 39, 41, 56, 57 and 59 are patentable under 35 U.S.C. 103(a) over Grawrock in view of U.S. Pat. No. 6,615,264 to Stoltz (hereinafter “Stoltz”).

Issue 4: Whether claims 22-23 and 60-61 are patentable under 35 U.S.C. 103(a) over Grawrock.

THE ARGUMENT

Issue 1: Whether claims 1-9, 11-19, 24-26, 28-37, 40, 42-55 and 58 are patentable under 35 U.S.C. 102(e) over U.S. Pat. No. 6,678,833 to Grawrock (hereinafter “Grawrock”).

In section 4 of the Office Action of August 15, 2006, the Examiner rejects Claims 1-9, 11-19, 24-26, 28-37, 40, 42-55 and 58 under 35 U.S.C. 102(e) as being anticipated by Grawrock. In particular, with respect to claims 1 and 6, the Examiner opines that Grawrock teaches the claimed (i) receiver for receiving an integrity metric because Grawrock’s “TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger” and cites to element 230 and cols. 2 and 4, (ii) integrity metric having

values for a plurality of characteristics associated with the computer entity because “examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system,” and (iii) controller for assigning a trust level to the computer entity from a plurality of trust levels wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric because Grawrock’s “TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level.” Appellants respectfully disagree and submit that while the Examiner’s interpretation is very broad indeed, it is far from reasonable in view of the plain language of Grawrock.

At the outset, Appellants wish to note to the Board that this case has followed a tortuous prosecution path that includes no less than four different Office Actions and one prior Appeal, all throughout which Appellants have gone far beyond the call of duty in trying to explain to the Examiner in ever-simpler words the differences between the prior art of record and their claimed invention. All these efforts have been met by nothing but ever-more creative “interpretations” of the prior art on the part of the Examiner that betray nothing beyond his singular dedication to (i) rejecting this application while (ii) never actually reading it, as proven by his often contradictory interpretations.

For instance, the Examiner’s present assertion that “examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system” is a complete turn-about from his interpretation set forth in the Office Action of March 7, 2006, wherein he asserted that the very same Grawrock reference teaches precisely the same integrity metric at col. 2 ll. 5-6 and col. 4 ll. 7-9 - i.e. “the hash value.” Erstwhile, as previously explained to the Examiner in a prior reply, the “hash value” taught by Grawrock at col. 2 ll. 5-6 is nonexistent (this passage discusses binding the TPM or Trusted Platform Module to a boot

memory block), and at col. 4 ll. 7-9 is limited to the following cryptic passage: “these modules 340, 350 and 360 can undergo a *hash operation* to produce corresponding identifiers 345, 355 and 365 for later use in verification by a challenger.” There is absolutely no mention anywhere else in Grawrock of these identifiers 345, 355 and 365. Presently, the Examiner has gone from alleging that the claimed “integrity metric having values for a plurality of characteristics associated with a computer entity” is anticipated by a *hash operation* to asserting that it is disclosed by any one of a plurality of *software modules*:

Similarly, during initialization, various *software modules* are provided to the TPM 230. Examples of the modules include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system that is loaded into the system memory 130 to control loading of the operating system. [Grawrock, col. 4 ll. 3-6, cited by the Examiner (emphasis added)]

With all due respect, Appellants submit that the Examiner’s assertion that software modules provided in a trusted platform module anticipate an integrity metric having values for a plurality of characteristics associated with a computer entity simply makes no sense, and the Examiner has wasted no time explaining how a software module can have values for a plurality of characteristics associated with a computer entity, much less point out specific support for this assertion in the actual disclosure of Grawrock.

As for the Examiner’s contention that “these integrity metrics also appear in the disclosure of the instant application” (emphasis in the original) at page 11 lines 10-15, this once again betrays the lack of attention on the Examiner’s part in perusing Appellants’ specification, as the cited portion merely lists rather standard components of a computing apparatus for which component configuration registers (CCRs) preferably are available. It is true that these CCRs can hold, *inter alia*, values that can be amassed into a digest to form the claimed integrity metric (as per Appellants’ disclosure), but there is certainly no such disclosure to be found in Grawrock.

The above notwithstanding, the Examiner’s final assertion that Grawrock discloses a controller for assigning a trust level to the computer entity from a plurality of trust levels wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric because the “TPM module reports the integrity metric upon the request

issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level” is the most erroneous of all. Claims 1 and 6 are clearly directed to an entity that is intended to reside between a user and a computer entity and which assigns a trust level to the computer entity based upon the integrity metric provided by the computer entity via its trusted device. There is no such entity disclosed in Grawrock. It is true that Grawrock teaches providing a computer entity with a trusted device (i.e. the TPM), and that the TPM can respond to a challenge with “identifiers 345, 355 and 365” so as “to determined that the platform has been initialized and is trusted.” [col. 4 ll. 36-38] However, there simply is no disclosure in Grawrock beyond this, and there is absolutely not one whisper in Grawrock of a computer apparatus that can challenge the TPM of a computer entity according to Grawrock and then, based upon its response, assign a trust level to that computer entity. “Determining” that a platform “is trusted” is not the same as “assigning a trust level” – “determining” is at most but one step of the process of “assigning” and, furthermore, even the Examiner’s invocation of a “broadest interpretation” does not render the disclosed option of trusted-or-untrusted anticipatory of the presently claimed *plurality of trust levels*. There is only one trust level disclosed in Grawrock – that is, “trusted.” The Examiner finds no support in Grawrock, Appellants’ specification, nor English common usage for his desire to render “not trusted” akin to a “trust level.” These are not mere semantic differences – the ability to assign one of a plurality of trust levels offers a much more flexible operating environment wherein various application programs can access various types of data depending on the trust level assigned to the computer entity in response to each user’s challenge; there is no such flexibility afforded by the system of Grawrock, which merely *informs* a user whether the platform is trusted or not.

Therefore, in view of all of the preceding, Appellants respectfully submit that claims 1 and 6 are in fact novel and nonobvious over the cited art, and request that the Examiner’s rejection of these claims be overturned on appeal.

Claims 2-5 depend from claim 1 and thus, in view of the above discussion, it is submitted that because claim 1 is allowable, claims 2-5 are also allowable at least by virtue of their dependency on claim 1.

With respect to claim 7, the Examiner largely repeats the rejections leveled at claims 1 and 6 and further asserts that Grawrock teaches the claimed comparing values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party because “the challenger that verifies and determines the trust level (i.e. trusted or un-trusted) is interpreted as the trusted party *that must provide the authentication values* for comparing against the integrity metrics reported by the TPM as that whether the platform is trusted or not can be determined accordingly.” Appellants submit that this assertion finds absolutely no support in the plain language of Grawrock. Where, for instance, does the Examiner find Grawrock offering any support for his interpretation that the challenger (i) is a *trusted* party, and (ii) *must* provide “the authentication values?” What “authentication values?” The answer is “nowhere.” There is one and only one sentence in Grawrock that discusses what a challenger is:

A "challenger" may be any electronic device within the platform or even external to the platform. [col. 4 ll. 11-12]

There is nothing in Grawrock that could possibly be understood as supporting the Examiner’s assertion that such a challenger is a trusted party, that it has “the authentication values” in its possession (not what “the authentication values” might be), or that it must provide the alleged authentication values for comparing against the integrity metrics allegedly reported by the TPM.

With respect to the balance of the Examiner’s allegations regarding Grawrock anticipating claim 7, Appellants refer to the above discussion of claims 1 and 6 and submit that this discussion is equally applicable to claim 7. Appellants thus respectfully submit that claim 7 is also novel and nonobvious over the cited art, and request that the Examiner’s rejection of this claim be overturned on appeal.

Claims 8-23 depend from claim 7 and thus, in view of the above discussion, it is submitted that because claim 7 is allowable, claims 8-23 are also allowable at least by virtue of their dependency on claim 7.

The Examiner’s rejection of claims 24 and 42 is predicated upon the Examiner’s arguments already addressed previously with respect to claims 1, 6 and 7, and Appellants therefore submit that the above discussion also fully supports the reversal of these rejections on

appeal. Appellants further note that claims 25-41 depend from claim 24 and claims 43-61 depend from claim 42, and thus submit that these claims are therefore also allowable at least by virtue of their dependencies.

Issue 2: Whether claims 10, 27 and 45 are patentable under 35 U.S.C. 103(a) over Grawrock in view of U.S. Pat. No. 6,209,099 to Saunders (hereinafter “Saunders”).

In section 5 of the latest Office Action, the Examiner rejects claims 10, 27 and 45 as being unpatentable under 35 U.S.C. 103(a) over Grawrock in view of Saunders. Claim 10 depends from claim 7, claim 27 depends from claim 24, and claim 45 depends from claim 42. “If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.” *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Thus, in view of the above discussion, it is submitted that because claims 7, 24, and 42 are allowable, claims 10, 27 and 45 are also allowable at least by virtue of their dependencies.

Issue 3: Whether claims 20, 21, 38, 39, 41, 56, 57 and 59 are patentable under 35 U.S.C. 103(a) over Grawrock in view of U.S. Pat. No. 6,615,264 to Stoltz (hereinafter “Stoltz”).

In section 6 of the latest Office Action, the Examiner rejects claims 20, 21, 38, 39, 41, 56, 57 and 59 as being unpatentable under 35 U.S.C. 103(a) over Grawrock in view of Stoltz. Claims 20 and 21 depend from claim 7, claims 38, 39 and 41 depend from claim 24, and claims 56, 57 and 59 depend from claim 42. Appellants thus submit that claims 20, 21, 38, 39, 41, 56, 57 and 59 are allowable at least by virtue of their dependencies.

Issue 4: Whether claims 22-23 and 60-61 are patentable under 35 U.S.C. 103(a) over Grawrock.

In section 7 of the latest Office Action, the Examiner rejects claims 22-23 and 60-61 as being unpatentable under 35 U.S.C. 103(a) over Grawrock. Claims 22-23 depend from claim 7, and claims 60-61 depend from claim 42. Appellants thus submit that claims 22-23 and 60-61 are allowable at least by virtue of their dependencies.

CONCLUSION

In view of the extensive reasons advanced above, Appellants respectfully contend that each claim is in fact novel and patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

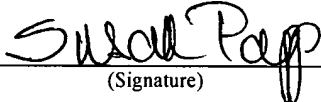
I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

January 2, 2007

(Date of Transmission)

Susan Papp

(Name of Person Transmitting)

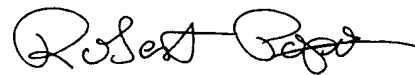


(Signature)

01/2/07

(Date)

Respectfully submitted,



Robert Popa

Attorney for Appellant

Reg. No. 43,010

LADAS & PARRY

5670 Wilshire Boulevard, Suite 2100

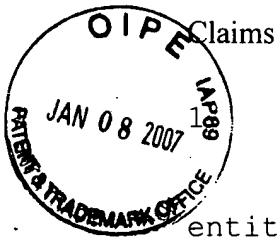
Los Angeles, California 90036

(323) 934-2300 voice

(323) 934-0202 facsimile

rpopa@ladasparry.com

Attachments



Computer apparatus, comprising:
a receiver for receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity; and
a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric.

2. Computer apparatus according to claim 1, wherein the trusted device is arranged to acquire an integrity metric of the computer entity.

3. Computer apparatus according to claim 1, wherein the trust level is determined by comparing the value of the at least one characteristics with a specified value.

4. Computer apparatus according to claim 1, wherein the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity.

5. Computer apparatus according to claim 1, wherein the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics for a plurality of computer entities.

6. A method of assigning a trust level, comprising:

receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity; and

assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric.

7. A method for establishing communications with a computer entity, comprising:

requesting a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity;

receiving a response from the trusted device including an integrity metric calculated for the entity by the trusted device;

comparing values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party; and

selecting a level of trust for the entity from a plurality of predefined levels of trusts based on at least one value in the integrity metric calculated for the entity by the trusted device.

8. The method of claim 7, wherein the trusted device is hardwired to the computer entity.

9. The method of claim 8, wherein the trusted device is configured to control the boot process of the computer entity.

10. The method of claim 9, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

11. The method of claim 8, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

12. The method of claim 7, wherein the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party.

13. The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity.

14. The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

15. The method of claim 14, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

16. The method of claim 15, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

17. The method of claim 15, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information.

18. The method of claim 12, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

19. The method of claim 12, wherein the response received from the trusted device includes the authenticated values provided by the trusted party.

20. The method of claim 7, wherein requesting the trusted device for the integrity metric comprises:

generating a nonce to pass to the trusted device with the request.

21. The method of claim 20, wherein the response from the trusted device includes the nonce received with the request.

22. The method of claim 7, further comprising:

initiating data transfer to the entity in accordance with the selected trust level.

23. The method of claim 22, wherein initiating data transfer to the entity in accordance with the selected trust level comprises transferring no data.

24. A method for a computer entity to respond to a request for integrity check prior to exchanging data, comprising:

receiving at a trusted device associated with a computer entity a request to provide an integrity metric containing values indicative of one or more characteristics of the entity;

calculating at the trusted device values indicative of one or more characteristics of the entity; and

providing a response from the trusted device including an integrity metric including the values indicative of one or more characteristics of the entity.

25. The method of claim 24, wherein the trusted device is hardwired to the computer entity.

26. The method of claim 25, wherein the trusted device is configured to control the boot process of the computer entity.

27. The method of claim 25, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

28. The method of claim 25, wherein the trusted device is

comprised of a plurality of components hardwired to the computer entity.

29. The method of claim 24, wherein the trusted device is configured to contain one or more of a public encryption key, a private encryption key, and one or more authenticated values provided for the entity integrity metric by the trusted party.

30. The method of claim 29, wherein the integrity metric includes one or more values calculated by generating a digest of BIOS instructions in the BIOS memory of the entity.

31. The method of claim 29, wherein the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity.

32. The method of claim 31, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

33. The method of claim 32, wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity.

34. The method of claim 32, wherein the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous

update information.

35. The method of claim 29, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

36. The method of claim 35, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

37. The method of claim 29, wherein the response further includes authenticated values provided for the entity by a trusted party.

38. The method of claim 29, wherein the request includes a nonce.

39. The method of claim 38, wherein the response includes the nonce received with the request.

40. The method of claim 29, wherein the request includes input data.

41. The method of claim 40, wherein the response includes the input data processed with the private encryption key.

42. A method for establishing communications between a computer entity and a user, comprising:

presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity;

presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device;

comparing at the user values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party; and

selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device.

43. The method of claim 42, wherein the trusted device is hardwired to the computer entity.

44. The method of claim 43, wherein the trusted device is configured to control the boot process of the computer entity.

45. The method of claim 44, wherein the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

46. The method of claim 43, wherein the trusted device is comprised of a plurality of components hardwired to the computer entity.

47. The method of claim 42, further comprising:
passing from the trusted party to the trusted device one or more
of a public encryption key, a private encryption key, and one or
more authenticated values for the entity integrity metric.

48. The method of claim 47, wherein the trusted device is
configured to calculate the integrity metric by generating a
digest of BIOS instructions in the BIOS memory of the entity.

49. The method of claim 47, wherein the trusted device is
configured to calculate the integrity metric by measuring one or
more values of configuration information regarding one or more
components of the entity.

50. The method of claim 49, wherein the components of the
entity are selected from among the group of components
comprising hardware components and software components.

51. The method of claim 50, wherein the components of the
entity are selected from among the group of components
comprising the BIOS, ROM, operating system loader, and operating
system of the entity.

52. The method of claim 50, wherein the configuration
information measured for at least one of the components
comprises one or more of certificate information, last update
information, latest update version information, and previous
update information.

53. The method of claim 47, wherein the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components.

54. The method of claim 49, wherein the components of the entity are selected from among the group of components comprising hardware components and software components.

55. The method of claim 47, wherein the response received from the trusted device includes the authenticated values provided by the trusted party.

56. The method of claim 42, wherein the request includes a nonce.

57. The method of claim 56, wherein the response includes the nonce received with the request.

58. The method of claim 47, wherein the request includes input data.

59. The method of claim 58, wherein the response includes the input data processed with the private encryption key.

60. The method of claim 42, further comprising:
initiating data transfer from the user to the entity in accordance with the selected trust level.

61. The method of claim 60, wherein initiating data transfer from the user to the entity in accordance with the selected trust level comprises transferring no data.

U. S. Appln. No. 09/931,526

Brief on Appeal dated January 2, 2007

In support of Notice of Appeal submitted November 14, 2006

Evidence Appendix Page B-1



There is no evidence submitted with the present Brief on Appeal.

U. S. Appln. No. 09/931,526

Brief on Appeal dated January 2, 2007

In support of Notice of Appeal submitted November 14, 2006

Related Proceedings Appendix Page C-1



There are no other appeals or interferences related to the present application.